Divailton Teixeira Machado
Aluno de Pós-graduação em crimes e perícias eletrônicas da UPIS
Sob orientação do professor
Laerte Peotta de Melo
Mestre em Engenharia Elétrica, Universidade de Brasília
Professor da UPIS

Recuperação de dados em *hard disk*

Considerações preliminares

O valor da informação para os negócios e para as pessoas nos dias de hoje é incalculável. Para os diversos setores da sociedade ela se apresenta como sendo tão valiosa quanto os bens de produção ou capital financeiro. Este artigo vai testar técnicas de recuperação de dados utilizando softwares comercialmente disponíveis.

A forma de utilização do meio magnético para armazenamento de dados em hard disk permite uma possibilidade de recuperação de dados. Isso se dá porque os sistemas operacionais, responsáveis pelas operações de processamento de um computador, utilizam um protocolo de armazenamento onde os dados, ou não são realmente apagados do hard disk, ou podem ser parcialmente apagados.

Mesmo com os dados sendo sobrescritos ainda existem teorias que demonstram a possibilidade de recuperar dados que supostamente foram apagados do hard disk, estas teorias não serão objetos de testes, mas alguns testes serão realizados para tentar comprovar a dificuldade de recuperar dados que foram sobrescritos. Manter a informação sempre a mão tem sido uma preocupação de muita gente, como podemos perceber na grande avalanche de sistemas de backup cada vez mais sofisticados e caros. Alguns autores como Petter Gutman[1] e Bruce Scheiner[2] tem postado artigos sobre a recuperação de informações gravadas em hard disk e como protegê-las. A proteção da informação é o cerne destes artigos, pois representa segurança para quem utiliza a informação como meio valioso. Com o surgimento do computador e sua expansão começou uma utilização generalizada deste recurso, de forma que o computador se tornou parte integrante de qualquer negócio. Os computadores, em sua maioria, possuem unidades de disco rígido para armazenamento de dados em massa e a recuperação destes dados em caso de sinistro, ou quando se necessita investigar algum acontecimento, lícito ou não, vem tomando atenção da comunidade científica e acadêmica.

O desenvolvimento da tecnologia de fabricação dos *hard disk*[3], tornou-o bastante acessível em termos financeiros ao mesmo tempo a capacidade de armazenamento vem aumentando vertiginosamente. Este efeito faz do *hard disk* uma oportunidade de armazenamento de dados bastante atrativa, pois o custo benefício é bom. Com este efeito não é difícil imaginar que a maioria dos computadores pessoais possui um *hard disk*, assim como os

[1] http://www.cs.auckland.ac.nz/~pgut001/pubs/secure_del.html - acesso em 01.01.08

[2] http://www.schneier.com/ - acesso em 01.01.08

[3] MORIMOTO, CARLOS E. **Manual de Hardware Completo 3º Ed. Pág. 149**. www.guiadohardware.net

servidores de serviços de computação. A utilização em massa de *hard disk* em computadores gera automaticamente uma confiança nos dados gravados neste tipo de mídia e é ai que a recuperação aparece como uma ferramenta para garantir a segurança em caso de perda de dados, seja intencional, ou por ação de terceiros, como é o caso dos vírus.
Grandes *hard disk´s* implicam em grandes volumes de dados que são gravados pelas pessoas, utilizando-se sistemas operacionais cada vez mais modernos, mas as técnicas de gravação de dados não tem sofrido modificações expressivas. Os fabricantes de sistemas operacionais, responsáveis pelos dados que são gravados nos *hard disk*, não tem feito modificações na forma em que os dados são distribuídos e gravados no disco. Apesar de existirem muitas formas de armazenagem lógica de dados elas não são novas e suas modificações nem sempre abandonam o método antigo. Os sistemas operacionais baseiam-se em sistemas de arquivos para poderem controlar como os dados serão alocados. Um dos mais utilizados é o *NTFS*[4] da *Microsoft corporation*. Ele foi criado para resolver alguns problemas de segurança de seu antecessor o FAT. O sistema *FAT* funciona como uma tabela em que os dados que serão gravados, ou re-gravados, possuam um endereço em uma tabela para que o sistema operacional possa administrar. O *NTFS*, também funciona a partir de uma tabela, um pouco mais moderna e funcional, mas o princípio de administração dos dados a serem gravados nos discos rígidos continua o mesmo. Existem ainda muitos outros tipos de sistemas de arquivo, como o *EXT2, EXT3, RAISERFS* e outros, mas o artigo vai tomar como exemplo o *NTFS*.
Algumas técnicas de recuperação de dados valem-se dos sistemas de arquivo para recuperar os dados, outras vão direto ao disco propriamente dito. Assim o teste apresentado neste artigo, por limitação de recursos, vai se fixar a utilização de softwares comerciais em versões *Trial* desenvolvidos exclusivamente para sistema operacional windows, onde eles que se propõe a recuperação de dados a partir de sistemas de arquivos *NTFS*.
Este artigo vai tratar, de maneira simples e linguagem didática, o funcionamento dos discos rígidos aqui denominados apena por *hard disk´s*, suas formatações física e lógica, técnicas de recuperação de dados utilizando programas comerciais acessíveis a todas as pessoas e apresentar, em linhas breves, algumas técnicas utilizadas para dificultar a recuperação de dados.

Funcionamento do *hard disk*

Para uma melhor compreensão das técnicas de recuperação de dados será apresentada, de forma simples e reduzida uma breve descrição do funcionamento básico dos *hard disk´s*, seus componentes principais, organização física e lógica do armazenamento de dados e sistemas de arquivos. Para uma melhor exemplificação será abordado o sistema de arquivos[5] *NTFS*.

Estrutura Física de um *hard disk*

O funcionamento de um *hard disk* dividir-se, basicamente, em três sistemas, abordando hardware de controle e conectividade, dispositivos eletro motores e elementos magnéticos.
Este conjunto de sistemas está interligado entre si e fazem ponte para o sistema operacional

[4] MORIMOTO, CARLOS E. **Manual de Hardware Completo 3º Ed. Pág.. 277**. www.guiadohardware.net

[5] MORIMOTO, CARLOS E. **Manual de Hardware Completo 3º Ed. Pag. 337**. www.guiadohardware.net

utilizar-se de suas funcionalidades.
O primeiro sistema que compõe o disco rígido é o eletromagnético. Este sistema é composto de bobinas eletromagnéticas e pratos, ou discos, metálicos feitos de alumínio. As bobinas funcionam como eletroímãs quando são submetidas a uma corrente elétrica aplicada nelas para que gerem um campo magnético nos pratos. Estas bobinas eletromagnéticas são comumente chamadas de cabeças de leitura e gravação. Os discos metálicos que recebem o nome de pratos são fabricados, geralmente de alumínio e recebem uma camada de material magnético, nas suas duas faces. O sistema também inclui os braços que suportam estas cabeças. A posição dos braços que suportam as cabeças de leitura e gravação não permite que estas se encostem aos discos, mas fiquem muito perto.
O segundo sistema é composto por motores e alavancas de precisão. Estes componentes ficam junto aos discos metálicos dentro do *hard disk* e são responsáveis por mover as cabeças, ou bobinas eletromagnéticas, para as áreas dos discos metálicos e fazer com que os eles girem em altíssima velocidade.
Um terceiro sistema é o eletrônico. Ele é responsável por converter os sinais eletromagnéticos em sinais digitais e vice-versa, além de outros controles como o acionamento correto dos motores e braços mecânicos e alimentação para os outros sistemas. É neste sistema que podemos observar as interfaces de comunicação que interligam a leitura dos dados com as requisições da CPU. Estas interfaces são conhecidas como *ide, ata, ultra ata,* e outros.

Formatação física do *hard disk*

A formatação física do *hard disk* é uma maneira de organizá-lo e prepará-lo para o uso. Esta etapa é realizada ainda no processo de fabricação e consiste em marcar fisicamente todo o disco, criando trilhas, setores e cilindros no disco rígido. As trilhas que vão desde o começo do disco (trilha zero) até o final, ficam divididas em partes, chamados de setores, que é a menor quantidade de espaço utilizável para armazenamento físico no *hard disk*, tradicionalmente o tamanho do setor fica em 512 bytes, mas é possível que o setor seja maior. Este artigo vai fixar seu estudo em setores de 512 bytes. O conjunto concêntrico de trilhas é denominado de cilindros. O processo de formatação física serve ainda para identificar locais em que não será possível contar com o bom funcionamento da superfície metálica magnetizada. Estes locais que não possuem bom funcionamento são chamados de b*adblock´s*. Com a marcação das trilhas, a formatação pode indicar como a divisão do disco esta disposta, e de posse destas informações é possível calcular o tamanho de armazenamento do *hard disk*. Estas informações são muito importantes, pois vão influir como as cabeças de leitura vão atuar. Como esta marcação é física, ou seja, os discos metálicos são marcados por equipamentos especiais, o processo de formatação física não pode ser desfeito ou refeito através de software. A de salientar que este processo de controle de áreas que não estejam em bom funcionamento é dirigido ao hardware dos discos mais modernos, mas já foi de responsabilidade do sistema operacional tal tarefa. Com as informações de quantidade de trilhas, setores por trilhas e quantos cilindros possui um *hard disk*, podemos calcular o espaço de armazenamento de um determinado disco com uma conta simples. O número de setores por trilha X número de trilhas X Quantidade de cabeças de leituras/gravação tudo isso multiplicado pelo número de bytes que cada setor possui. Vejamos um exemplo hipotético de um *hard disk* que tenha 16383 cilindros, 16 cabeças e 63 setores por trilha e que o setor seja de 512 bytes. Este disco terá uma capacidade de armazenamento de:
16383x16x63=16514064 X 0,5 (meio Kb) = 8257032 kbytes ou **8,25 MB.**

Formatação lógica do *hard disk*

O *hard disk*, após o processo de formatação física, fica apto a uma organização lógica. Esta organização pode ser entendida como uma formatação lógica, em que o hardware (placas de alumínio, magnetizadas, divididas e devidamente endereçadas) pode agora ser utilizado para guardar dados, de forma organizada. A formatação lógica cria a maneira com que os dados serão armazenados no disco e esta maneira diz como vamos dividir o disco, criando partes, ou como são comumente chamadas: partições. Estas partes lógicas de um mesmo disco físico receberão o nome de volumes. Um conjunto de setores será definido como uma pequena unidade que recebe Ra os dados e os armazenará conforme um modelo. Este conjunto de setores físicos pode ser denominado de várias maneiras, dependendo do tipo de sistema de arquivos utilizado para as partes lógicas, no caso do sistema de arquivos *ntfs* este conjunto denomina-se cluster[1]. Em outros sistemas de arquivos estes conjuntos de setores recebem nomes diferentes como no caso do *EXT2*, onde eles se chamam *Inode´s*[6].

Sistema de arquivos

Um sistema de arquivos é um conjunto de rotinas e estruturas lógicas, implementadas quando se realiza uma formatação lógica em um *hard disk*, capaz de auxiliar o sistema operacional no armazenamento de dados. Atualmente existem mais sistemas de arquivos que sistemas operacionais. Para ilustrar alguns testes, será utilizado o sistema de arquivos *NTFS*, da Microsoft.
O *ntfs* (sistema de arquivos da nova tecnologia) foi criado pela Microsoft para utilização em seus sistemas operacionais. Teve como seu antecessor o fat32 e trouxe facilidades como criptografia de arquivos e pastas e implementação de controle de acesso a arquivos. Tais recursos oferecem um nível maior de segurança quando comparado ao fat32. É um dos sistemas de arquivos mais utilizados no mundo. Seu funcionamento baseia-se em uma tabela mestre de arquivos a MFT, que regula onde os arquivos serão gravados. É nesta tabela que estão gravados os metadados dos arquivos. Metadados são informações complementares dos arquivos, como data de criação, privilégios de acesso, última modificação, localização física no disco, proprietário e outras informações referentes ao arquivo. Na tabela *MFT* estão armazenadas informações sobre todos os arquivos que estão gravados no disco, inclusive seus atributos. Além da *MFT* o sistema de arquivos *ntfs* cria outros diretórios para implementar a estrutura de controle do *hard disk* são eles:

$ AttrDef, Tabela definições de atributo: contém a definição de todos os atributos User-defined sobre o volume e sistema.
$BadClus, arquivo de cluster defeituosos: contém todos os o incorreto clusters no volume.
$ Cluster Allocation Bitmap: contém o bitmap para o volume inteira, mostrando quais clusters são usados.
$, Boot File: contém inicialização o volume do se o volume é inicializável.
$ LogFile, arquivo de log: usado para fins recuperação.
$ MFT, tabela de arquivos mestre (*MFT*): contém um registro para cada arquivo no volume *NTFS* no seu atributo de dados.
$ MftMirr, Tabela2 arquivo mestre (*MFT2*): espelho da *MFT* usado para fins recuperação.
$Cota , tabela de cota: tabela usada para indicar o uso de cota disco para cada usuário em

[6] MORIMOTO, CARLOS E. **Manual de Hardware Completo 3º Ed. Pag. 217**. www.guiadohardware.net

um volume.[7]

Com base nas informações gravadas nestes arquivos é possível recuperar dados que estavam gravados em um disco e foram apagados. A *MTF* registra em uma tabela, quais locais do *hard disk* estão disponíveis para uso. Alguns dos dados gravados são referentes à condição de um determinado arquivo, esta condição pode indicar que ele foi apagado, o que libera o espaço que o arquivo utilizava disco para ser utilizado novamente, ou ativo o que impede o sistema de gravar dados naquela localização para não haver sobreposição de dados. E com base nestas informações existe a possibilidade de recuperação de dados em *hard disk*.
A partir da técnica que o sistema de arquivos utiliza para gravar os dados no *hard disk* é possível recuperar dados apagados através de softwares que possuam capacidade de acesso a tabela de arquivos. A recuperação de dados através do acesso ao disco por software pode acontecer de duas formas. A primeira forma é renomeando os arquivos que foram apagados. O *NTFS* renomeia os arquivos que foram apagados de maneira que o sistema operacional não mais os identifique, e o sistema de arquivos possa liberar o espaço utilizado para outro arquivo. Com um acesso a Tabela mestra de arquivos é possível procurar os arquivos que estão apenas marcados como apagados e renomeá-los, fazendo com que voltem a ter o status de ativos.
A segunda forma é através do slack space. O slack space se dá quando um arquivo de tamanho maior é gravado primeiro e o sistema de arquivos o marca como sendo apagado e utiliza seu espaço para gravar um arquivo de tamanho menor. A diferença de espaço utilizado pode conter pedaços do arquivo que fora apagado e com acesso direto a tabela mestra de arquivos e ao disco é possível copiar o espaço que se encontra nesta diferença de tamanhos para uma área nova do disco tendo assim um arquivo novo, mas que corresponde a apenas parte do que foi apagado.

Teste – recuperação de arquivos apagados

Foi realizado um teste com alguns softwares comerciais que se propõe em recuperar arquivos apagados**.** Todos eles trabalham com a mesma técnica: acesso a tabela mestra de arquivos e ao disco valendo-se de busca a arquivos que foram marcados como apagados ou sobrescritos por arquivos de tamanhos menores.

Softwares utilizados

Para testar uma recuperação de arquivos foram utilizados três programas desenvolvidos para plataforma Windows, comercialmente divulgados e com suas versões Trial disponíveis para download nos sites dos fabricantes. São eles o EasyRecovery Professional Trial[8], GetDataBack for *NTFS*[9] Version 3.63 e Undelete Plus V. 2.97 completo[10]. Todos propostos como com capacidade de recuperação de dados apagados em sistemas de arquivos *NTFS*.

[7] http://support.microsoft.com/kb/103657/pt-br - acesso em 01.01.08

[8] http://www.ontrackdatarecovery.com/ - acesso em 01.01.08

[9] http://www.runtime.org/ - acesso em 01.01.08

[10] http://www.touchstonesoftware.com/ - acesso em 01.01.08

Metodologia dos testes.

Os testes foram realizados em um *hard disk* Toshiba Modelo MK2018GAP, acessado através de gaveta externa com comunicação USB e sobrescrito com zero lógico utilizando-se o seguinte comando linux: dd if=/dev/zero of=/dev/sdb1. Após a gravação de zero lógico em todo o *hard disk*, este foi formatado utilizando-se o Microsoft windows explorer com sistema de arquivos *NTFS* e tamanho de Cluster padrão. O sistema operacional utilizado para a instalação dos programas e realização dos testes foi o Microsoft windows vista home basic instalado em um notebook com processador Intel Pentium Core 2 duo 1,47 Ghz com 1 Gb de memória Ram.
Foi criado um arquivo no *hard disk* do tipo texto (.txt) e gravado a seguinte expressão : abcdefgh 12345678 em seu conteúdo. O arquivo foi gravado na pasta .\testes_Upis\arquivoteste.txt. Para criar o arquivo foi utilizado o Microsoft windows explorer programa nativo do sistema operacional windows . Após a criação do arquivo este foi deletado utilizando-se dois métodos:

Caso 01 – Seleciona-se o arquivo no Microsoft windows explorer e aperta a tecla delete.(envio do arquivo para lixeira do windows)

Caso 02 – Seleciona-se o arquivo no Microsoft windows explorer e aperta-se as teclas shift+delete simultaneamente.
Após cada um destes procedimentos executa-se os programas de recuperação.
Após o teste, novamente foi utilizado o comando dd do linux, para reescrever zero lógico em todo *hard disk*. Novamente foram executados os programas para recuperação de dados.

EasyRecovery Professional Trial

Software de recuperação de dados da empresa Ontrack, possui interface gráfica e se dispõe a recuperar arquivos deletados de uma pasta ou de discos que foram formatados.
Possui, ainda, opções para corrigir arquivos que estejam corrompidos do microsoft word, microsoft Excel, microsoft PowerPoint e MSAccess. As opções de recuperação de dados são: Partições formatadas, arquivos deletados, discos sem nenhuma estrutura de sistema de arquivos e dados gravados em uma sessão do sistema.

GetDataBack for *NTFS* Version 3.63

Software de recuperação de dados da empresa RunTime. Propõe-se a recuperar arquivos de partições lógicas formatadas, arquivos apagados acidentalmente ou por ação de vírus. Existem versões para outros tipos de sistemas de arquivos. As opções de recuperação de arquivo são: arquivos apagados, discos formatados, problemas causados por bad blocks e problemas causados pela interrupção de fornecimento de energia.

Undelete Plus V. 2.97 completo

Software de recuperação de arquivos da empresa Touchstone. O programa se propõe a recuperar dados apagados em todos os sistemas de arquivos de sistemas operacionais windows. Programa grátis e possui as seguintes opções de recuperação: apenas arquivos deletados. O fabricante indica que arquivos menores possuem maior probabilidade de ser recuperado quando comparados a arquivos maiores.

Resultados:

	GetDataBack for *NTFS* Version 3.63	Easy Recovery Professional Trial **l**	Undelete Plus V. 2.97 completo
Caso 01	Houve recuperação*	Houve recuperação	Não houve recuperação
Caso 02	Houve recuperação	Houve recuperação	Houve recuperação**
Após Zero Lógico	Não houve recuperação	Não houve recuperação	Não houve recuperação

* Houve a recuperação do arquivo, mas este veio com o nome $94D1.txt.
** Houve a recuperação de dois arquivos (Gravados em um pen drive):
E:\Estudo-UPIS\UndeletePlus_recuperados\testes_Upis\arquivoteste.txt.txt
E:\Estudo–UPIS\UndeletePlus_recuperados\$RECYCLE.BIN\...\$I8ATO6Z.txt

Análise dos testes: Primeiramente cabe salientar que para o primeiro caso não há ainda uma ação de apagar o arquivo do disco propriamente dita. O sistema operacional microsoft windows, vale-se de um recurso de segurança que consiste em mover o arquivo apagado com um delete simples, para uma pasta especial com o nome de *RECYCLER*, sendo possível restaurá-lo para sua pasta original sem a necessidade de softwares de terceiros.
Todos os programas foram executados com privilégios da conta administrador do sistema operacional windows vista.
Como resultado entre os programas de testes aplicados aos dois casos, o programa GetDataBack for *NTFS* Version 3.63, mostrou-se melhor para a recuperação de dados apagados do disco. Nos dois casos iniciais foi possível a recuperação de dados, ainda que com o nome do arquivo diferente. O programa ainda possui uma opção de log das ações realizadas, e traz muitas informações sobre o disco que está sendo alvo da recuperação, inclusive o número de série, label e proprietário.
Para os três programas analisados, nenhum conseguiu recuperação após aplicação de zero lógico em todo o *hard disk*.

Recuperação através de microscopia de força magnética (MFM) [11]

No teste realizado nenhum programa conseguiu recuperar dados após o disco ser reescrito com zero lógico. Isso se dá porque os programas estão baseados nas informações do sistema de arquivos, que apenas marca o arquivo como apagado e libera o espaço que antes o pertencia para que possa ser utilizado por outro arquivo.
Existe uma técnica que pode resolver o problema de recuperação de dados que foram sobrescritos é a Microscopia de força magnética.
O microscópio de força magnética é uma variante da microscopia de força atômica[7]. Consiste em um aparelho que com uma agulha aproximada de uma superfície magnética pode verificar o campo magnético com bastante precisão. Uma análise precisa do campo magnético gera a possibilidade de comparar os valores medidos pela microscopia de força magnética com valores padrões de gravação de dados. É esta comparação que torna possível a recuperação de dados sobrescritos. Essa funcionalidade se dá, porque na verdade, quando uma cabeça de gravação grava "1" por cima de um local onde antes era "0", existe uma pequena variação magnética. E quando a cabeça de gravação grava um "1" por cima de outro "1", também existe uma pequena variação que pode ser medida e com isso pode-se reconstruir os dados apagados[9]. Com as cabeças de leituras convencionais esta diferença é desprezada, mas com um microscópio magnético é possível detectar a variação

[11] http://www.cbpf.br/~nanos/Apostila/47.html - acesso em 01.01.08

magnética.

Técnicas de destruição de dados

Técnica de destruição de dados tem o objetivo de impedir sua recuperação. Vários setores da sociedade valem-se da computação para o tratamento de informações que muitas vezes são valiosas e precisam de um tratamento de armazenagem adequado ao seu valor. Pudemos perceber que o recurso de recuperação de dados está disponível em diversos sites da internet, facilitando cada vez mais a recuperação de dados. Quando uma informação precisa ser apagada de forma definitiva, é necessário que técnicas especiais de destruição de dados sejam aplicadas. O departamento de defesa dos estados unidos propõe um modelo de destruição de dados na recomendação DoD 522.22M[12], onde afirma que caso os dados sejam secretos as mídias de armazenagem devem ser incineradas, pulverizadas ou desintegradas. Alguns pesquisadores como Peter Gutmann e Bruce Schneier, além de algumas agências de inteligências de alguns países, propõe métodos para uma deleção de dados segura.

Algoritmo de Peter Gutmann

Peter Gutmann, cientista da computação do Departamento de Ciência da computação da universidade de Auckland, Nova Zelândia. Ele apresentou o artigo "Secure Deletion of Data from Magnetic and Solid-State Memory", para demonstrar que mesmo sobrescrevendo os dados em um disco rígido, a microscopia de força magnética ainda pode recuperar os dados. Para resolver este problema ele propõe uma série de sobrescrita de dados no *hard disk*, como forma de impedir a recuperação de dados. Sua técnica possui 35 passos, ou 35 seqüências de "0" e "1" lógicos que devem ser sobrescritos no *hard disk* a fim de impedir que dados úteis possam ser recuperados. Em outro artigo "Levantamento sobre a utilização de técnicas de microscopia na recuperação de dados em discos rígidos" [13] apresentado no evento iccyber2004[14] pelos Alexanders T. das N. Belarmino, Átila Leite Romero, Gustavo Scarpellini de Mello, Marcelo de Azambuja Fortes e Rafael Saldanha Campell, todos peritos criminais, existe citação de outros autores, mais especificamente Simson Garfinkel, Abhi Shelat e Daniel Feenberg que questionam a tese de Gutmann à vista da recuperação de dados em grandes volumes utilizando microscopia de força magnética, mas nada falam de pequenos volumes.

[12] https://www.dss.mil – acesso em 01.01.08

[13] http://www.iccyber.org/2007/Archive/ProceedingsICCyber2004.pdf - acesso em 01.01.08

[14] http://www.iccyber.org/ - acesso em 01.01.08

Considerações finais

A recuperação de dados é muito importante para várias áreas da ciência. Primeiro que em caso de desastre existe uma possibilidade de recuperação dos dados gravados em *hard disk* e segundo apresenta-se como uma segurança a mais na preservação da informação. O método utilizado para gravação dos dados em *hard disk* oferece dificuldade para se livrar dos dados. Muitos pesquisadores estão debruçados neste assunto, visto ser de grande impacto para o tratamento da informação em qualquer área. Para quem utiliza computadores pessoais e não possuem informações muito críticas podem contar com os programas comercialmente desenvolvidos para uso pelo próprio usuário. Quando é necessário uma recuperação de dados com a utilização de hardware, como é o caso da microscopia de força magnética, não é usual que o próprio usuário realize este procedimento, sendo necessário a interferência de terceiros, seja de maneira comercial, como é o caso das empresas especializadas em recuperação de dados, seja de maneira acadêmica com o auxílio das universidades. Em ambos os casos é necessário investimento financeiro mais elevado. O assunto foi abordado de maneira superficial e simples, carece de aprofundamento, principalmente para o desenvolvimento de ferramentas de recuperação de dados que atenda a usuários domésticos e investigações acerca do fenômeno magnético presente nos *hard disk´*s. Partindo de um princípio de que a informação deve ser de acesso livre a todos, fica aqui uma oportunidade e um apelo para a comunidade científica e acadêmica desenvolver o tema.

Referências:

FARMER, DAN. **Perícia Forense Computacional** /Dan Farmer, Wietse Venema; Tradução Edson Furmankiewicz, Carlos Shafranski, Docware Traduções Técnicas; revisão técnica Pedro Luis Próspero Sanchez. – São Paulo: Pearson Prentice Hall, 2007.

FREITAS, ANDEY RODRIGUES DE. **Perícia Forense aplicada à informática**; ambiente Microsoft / Andrey Rodrigues de Freitas. – Rio de Janeiro: Brasport, 2006.

CARRIER, BRIAN. **File System Forensic Analysis**. USA : Addison Wesley, 2005.

MORIMOTO, CARLOS E. **Manual de Hardware Completo 3º ed**. www.guiadohardware.net

TORRES, GABRIEL**. Hardware curso completo 3ª edição**. Gabriel Torres. Axcel Books, 1999.

http://www.microsoft.com - acesso em 01.01.08

http://www.peotta.com - acesso em 01.01.08

http://support.microsoft.com/kb/103657/pt-br - acesso em 01.01.08

Resumo

Este artigo demonstra singelamente o funcionamento de um *hard disk*, propõe um teste para recuperação de dados apagados em um sistema de arquivos *NTFS* e faz uma simples avaliação de algumas técnicas utilizadas para impedir a recuperação de dados. Foram utilizados alguns softwares comerciais em suas versões *Trial*, utilizados para recuperação de dados apagados em *hard disk* e ao final foi realizado um comparativo entre eles.

Palavras-chave: *hard disk*, dados, recuperação